2010

IBA Performance and Usability for Mobile Phones

Yeah Teck Chen
University of South Australia, YeahTeck.Chen@postgrads.unisa.edu.au

Gaye Lewis
University of South Australia, gaye.lewis@unisa.edu.au

IBA Performance and Usability for Mobile Phones

Yeah Teck Chen
School of Computer and Information Science
University of South Australia
Australia
Email: YeahTeck.Chen@postgrads.unisa.edu.au

Gaye Lewis
School of Computer and Information Science
University of South Australia
Australia
Email: Gaye.Lewis@unisa.edu.au

Abstract

Mobile phones are becoming increasingly sophisticated, enabling consumers to access more services and generate more data. However, the current PIN and password protection capabilities available on mobile phones are often misused resulting insufficient protection of the information stored within mobile phones. Image-based authentication (IBA) leverages the human ability to recognize graphics better than recalling a sequence of strings and results have shown increased pass-image memorability among users. In this paper, the performance results and user opinions of two IBA techniques, Picture Password and Awase-E, will be compared alongside PIN and password as control techniques. In summary, of the data on authentication speed and success rate were collected but results indicate that Awase-E is possibly a superior technique which is more preferred by users.

Keywords

Mobile, Image-based Authentication, Performance, Usability, Picture Password, Awase-E

INTRODUCTION

A standard mobile phone normally comes with a simple device power-on PIN protection while more advanced models may include PIN authentication for waking from inactivity. However, research has shown that 34% of users disabled the PIN while the remaining 66% did not use it properly (Clarke and Furnell 2005), resulting in insufficient protection of information stored within mobile phones.

Although a significant amount of research has been conducted to improve the security of PIN and password systems, the focus of the research has always been on designing new technical methods to authenticate users, rather than examining the usability of those methods (Adams and Sasse 1999). While advanced authentication systems such as token-based and biometrics exist, these systems are well known for their drawbacks, including requiring extra hardware, increased implementation cost and accuracy issues (Grashey and Schuster 2006; Nicholson et al. 2006). Often, these authentication systems implement some level of PIN or password based mechanism for initialization or "fallback" or as a secondary authentication method.

Image-based authentication (IBA) research, which leverages the human ability to recognize graphics better than recalling a sequence of strings and numbers showed promising results with the improvement in memorability of pass-images as seen in Awase-E (Takada et al. 2006). Most of the input methods for IBA techniques are similar to PIN and password systems, thus adoption of such systems is more likely to succeed due to a lower learning curve, considering that PIN and password systems are still the most commonly used mechanisms for user authentication on a mobile phone. However, IBA techniques are not without drawbacks as they tend to yield higher authentication times (Dhamija and Perrig 2000) and other input errors such as incorrect sequence and double selection (De Angeli et al. 2003). To date, IBA techniques have always been compared against PIN and password.

This paper reports on the results of an experiment conducted to compare two IBA techniques, Picture Password (Jansen 2004) and Awase-E, with PIN and password used as control techniques. By investigating the performance, in terms of authentication speed and success rate, and the user opinions of these techniques, usability issues are identified leading to design suggestions to improve these techniques. This paper begins with some background on user authentication and image-based authentication and then outlines the research methodology employed in the experiment. Findings are discussed and the conclusion presents potential improvements for IBA techniques and directions for future research.

BACKGROUND

User authentication is a process to verify the identity of a person which is a vital mechanism employed to protect assets and more importantly, access to data and resources. There are generally three approaches (O'Gorman 2003) for authenticating users and they are:

(a) Knowledge Based – that are dependent on "something the user knows" such as a PIN or password. However, compared to laptops, mobile devices are used more frequently to perform shorter tasks and require instantaneous access. Troublesome authentication such as PIN and password gets disabled when there are no policies enforcing their use (Phifer 2008). Research also shows that users may use the default PIN, forget their PIN or neglect to change their PIN (Clarke and Furnell 2005) while some users may record their PIN or password in one form or another (Adams et al. 1997).

(b) Object Based – is reliant on "something that the user possesses" such as a token or smart media (MMC, SD, etc). The token normally stores information such as keys and digital certificates that proves that the token is valid and is usually hard or impossible to forge (Phifer 2008). However, tokens are often left in situ for the sake of convenience, as with the Subscriber Identity Module, more frequently known as the SIM card. They may be forgotten or lost and the implementation of tokens is costly in terms of extra hardware.

(c) ID Based – leverages unique attributes of a person or "someone who the user is" such as his or her physical attributes or behaviour. Authentication of this type is called biometric authentication and it uses sensor devices to capture a user's biometrics such as fingerprints, to be compared with samples that have been provided earlier. However, biometrics also requires extra hardware with associated costs for implementation. Another well known challenge of biometric authentication is the accuracy issues that are associated with two types of errors: false acceptance rate (FAR) and false rejection rate (FRR) (Furnell and Clarke 2007). Noise during data capture may also reduce the accuracy of these systems.

IMAGE-BASED AUTHENTICATION

IBA techniques aim to improve on the memorability of PIN and password systems by replacing them with graphics and photos. The logic behind these techniques is that humans can generally recognize better than they can recall, as argued Nielsen in 1993 (Dhamija and Perrig 2000). The research into IBA techniques can be grouped into two distinctive categories.

(a) Recognition based techniques, which is the main focus of this research, use images, photographs or icons to stimulate user's recognition ability during the authentication process. The user may not be able to explicitly remember the graphics, but prompts using the selected images help the user to recognize and pin point them.

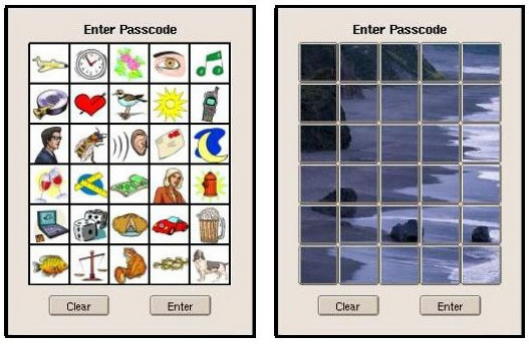


Figure 1: Two distinctive authentication styles of Picture Password (Jansen 2004).

The Picture Password technique presents users with a group of images that can be made up of photos, icons, or parts of a photo (Refer to Figure 1). During authentication, users will need to point out, in sequence, the previously selected images for authentication.

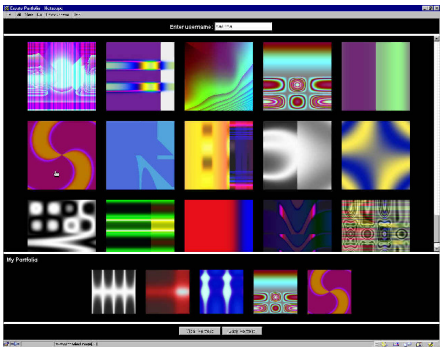


Figure 2: Examples of graphics used as pass-images in Déjà vu (Dhamija and Perrig 2000).

A variation of this technique called Déjà vu (Refer to Figure 2) uses random art in place of the icons or images. However, the technique requires the input of username and selection of previously recorded pass-images from among decoy images and is more suitable for devices with keyboard entry and screen sizes such as ATM or Web applications.

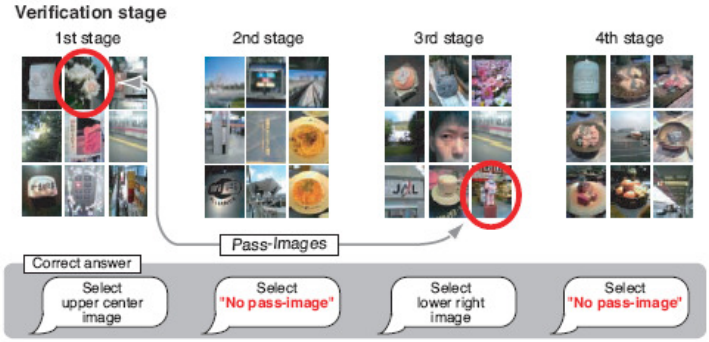
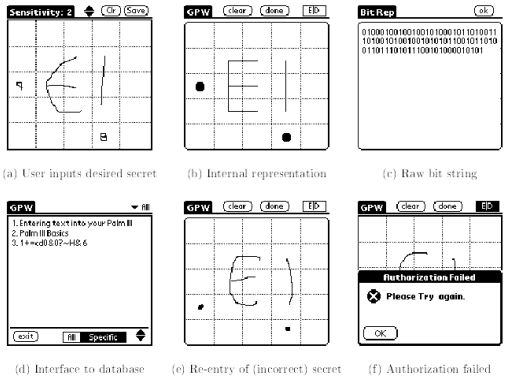


Figure 3: Verification stages in Awase-E (Takada and Koike 2003).

Awase-E (Refer to Figure 3) presents users with a similar user interface but uses a slightly different approach for authentication. Users need to choose or enrol at least one pass-image. During the authentication process, users are presented with 4 sets of images which include decoy images. The users have to find and point out their pass-image and if they don't see their pass-image, they have to select a "No pass-image" button, and then the next set of images will be presented, and so on. The technique randomizes the number of pass-images, the position of images, and the image set in which the enrolled pass-image is located for each authentication round.

(b) Recall based techniques are similar to the biometric signature technique, requiring the recall of graphics that are created by the user. These graphics can be in the form of shapes, drawings or a signature. The idea is that no visual stimuli will be given and the user needs to specifically remember and reproduce the previously created graphics.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Figure 4: Draw-a-secret (DAS) authentication process (Jermyn et al. 1999).

The DAS technique (Refer to Figure 4) records the coordinates, sequences and directions of the pen strokes drawn by a user on the 2D grid. To authenticate, the user has to reproduce the drawing on the same grid.

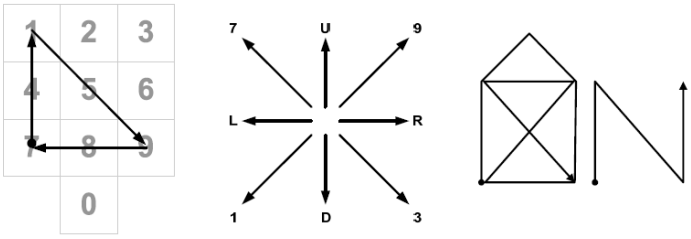


Figure 5: Left: Using shape to remember PIN 7-1-9-7, Middle: Stroke direction and the internal value interpreted by PassShape, and Right: Strokes interpreted as U93DL9L3XI3U with X as a padding value for multiple drawing (Weiss and Luca 2008).

Another recall based authentication technique is PassShape that uses stroke directions and sequences that produce certain shape such as a triangle for remembering PIN (Refer to Figure 5). A more advance version of this technique allows user to draw the shapes on a touch screen for authentication.

IBA Performance

The IBA performance aspects investigated in this research are authentication speed and success rate and the data collected from research participants are used to deduct usability issues of the investigated IBA techniques.

Currently, there has been no literature found that discusses performance in terms of authentication speed and success rate for Picture Password. The literature to date mainly describes the mechanism and entropy of the technique.

On the other hand, Awase-E has several reports that extensively discuss the authentication success rate of the technique, which were reported to be as high as 100% even after an experiment period of 16 weeks (Takada et al. 2006). However, authentication speed is not usually touted as one of the strengths of the technique as it was briefly reported that Awase-E authenticates at an average of 24.6 seconds (Takada et al. 2006).

RESEARCH METHODOLOGY

Selecting IBA Techniques to Evaluate

In this experiment, Picture Password and Awase-E will be compared alongside PIN and password to test their performance in terms of memorability and usability. In terms of design, both these techniques are quite different (Refer to Table 1) and it is worth comparing their performance side by side.

Table 1. Design differences between Picture Password and Awase-E

Picture Password	Awase-E
Tested on PDA	Tested on mobile phone
One screen authentication	Multiple screen authentication
Pass-image input sequence important	User pin points randomly placed pass-image across 4 screens
Uses thumbnails of multiple images randomly placed in a 5 x 6 grid	Uses thumbnails of multiple images randomly placed in a 3 x 3 grid
Select at least 4 pass-images	Select at least 1 pass-image

These two IBA techniques were selected for investigation because their input methods for authentication are comparable to each other and also similar to PIN and password where input is done by pressing on images arranged in a grid. Similar and familiar input and interaction may result in higher user acceptance. In contrast, DAS and PassShape and several other IBA techniques have very different input mechanisms.

Data Collection

For the purpose of data collection, a prototype implementing each authentication technique was developed and programmed using the .NET Mobile Platform. The prototype was deployed and tested on the same touch screen smart phone for each part of the experiment to enable all techniques to be evaluated equally. The prototype enabled collection of data on task completion time and error rate.

The data collection involved 20 test subjects of varying and balanced age, gender, educational level and knowledge of authentication. Each participant was asked to authenticate all techniques which were presented in random order. The experiment consisted of 3 stages:

(a) Stage 1: Enrolment and learning

Participant was given a brief introduction to the experiment and was asked to try each technique's enrolment and authentication in a demo mode where no data were collected. Then, they were asked to enrol themselves and offered several authentication rounds for learning.

The minimum length for the PIN is 4 digits and 6 characters for password, and they should be a combination that the participants believe to be safe and have never been used before. Picture password requires at least 4 pass-images while Awase-E requires at least one pass-image.

(b) Stage 2: Survey and Memory Test 1

Following the previous stage, the participant was asked to complete a questionnaire related to their behaviours and opinions towards mobile authentication and the tested IBA techniques. This questionnaire served as an unrelated task to distract the participants. After the completion of the questionnaire, which took around 15 to 20 minutes, the participant was asked to perform another authentication round.

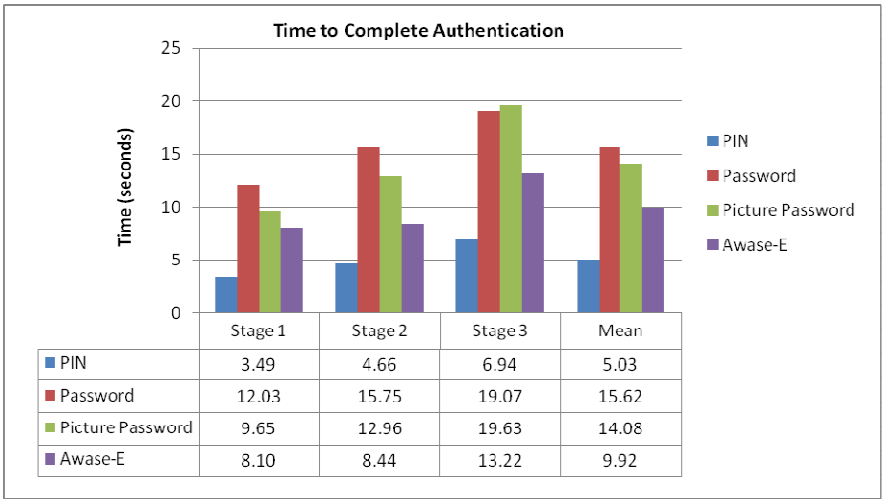
(c) Stage 3: Memory Test 2

For stage 3, the participant was requested to return a week later to perform another authentication round with the opportunity to retry as many times as required until authenticated successfully, or until they give up. Following the memory test, the participant was asked to complete a brief questionnaire to obtain their post experiment views and perceptions on the tested IBA techniques.

FINDINGS

In this section, both the quantitative and qualitative data collected from the prototype and user survey are presented in an integrated approach to discuss the performance and usability of the IBA techniques studied. Findings on authentication speed are presented first, followed by the findings on authentication success rate and finally, the user behaviour and opinions towards mobile security and IBA is discussed. In the last section, the issues and improvement areas for Picture Password and Awase-E are addressed.

Authentication Speed



	Stage 1	Stage 2	Stage 3	Mean
PIN	3.49	4.66	6.94	5.03
Password	12.03	15.75	19.07	15.62
Picture Password	9.65	12.96	19.63	14.08
Awase-E	8.10	8.44	13.22	9.92

Figure 6: Authentication speed for PIN, password, Picture Password and Awase-E

As expected, Figure 6 shows that PIN took the shortest time to authenticate, with participants averaging approximately 5 seconds in all stages. While its speed experienced marginal decrease over the duration of the experiment, PIN remained significantly faster than the other techniques. Interestingly, the performance of password was slower by at least two and up to three times when compared to PIN, recording an average authentication time of 15.62 seconds.

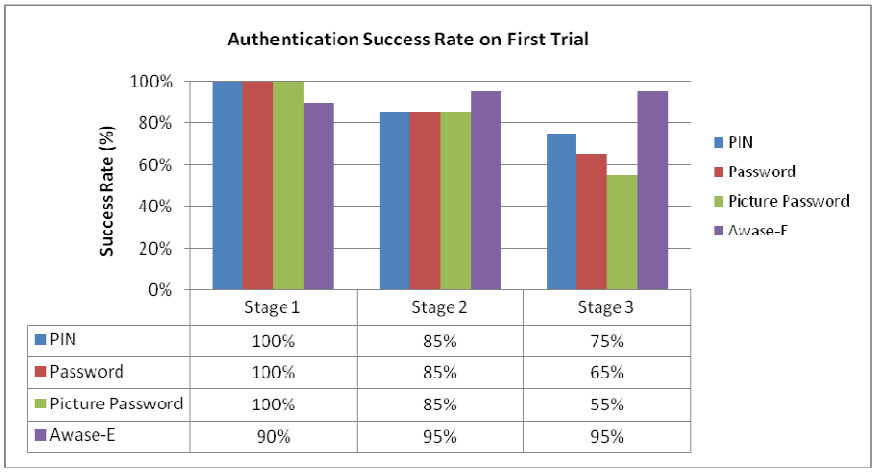
Picture Password authentication was quicker than password by a small gap in Stages 1 and 2 but unexpectedly slowed much to match password speed in Stage 3, averaging approximately 14 seconds in all stages. Perhaps the

most surprising result was that Awase-E, in contrast with the predicted result, came in second in terms of authentication speed, considerably and constantly authenticating faster than password and Picture Password, recording an average of a little less than 10 seconds.

The Picture Password authors had never published test results in terms of speed of authentication for the technique but this experiment shows that picture password is indeed a rather slow technique, in contrast with the earlier predicted outcome. Awase-E on the other hand, was reported to perform at an average of 24.6 seconds (Takada et al. 2006), which shows a huge gap with the performance results achieved in this experiment that recorded Awase-E authenticating at an average of 9.92 seconds. As the Awase-E authors (Takada et al. 2006) had not provided much information relating to the speed of authentication, it can only be speculated that perhaps most of the participants in the previous experiment used more than 1 pass-image resulting in a slower authentication speed, in contrast with the majority of participants in this experiment who used only 1 pass-image.

Again, personal devices such as mobile phones require instantaneous access (Phifer 2008) and in this case users seeking convenience may still prefer to use PIN simply because it is the fastest technique. However, some participants suggested that mobile phone users may be willing to tolerate slower authentication techniques such as password, Picture Password and Awase-E as long as it is deemed more secure, especially in the scenario where they are required to authenticate only once or several times in a day. Users that prefer to be authenticated every time they access the phone may be put off by slow authentication techniques.

Authentication Success Rate



	Stage 1	Stage 2	Stage 3
PIN	100%	85%	75%
Password	100%	85%	65%
Picture Password	100%	85%	55%
Awase-E	90%	95%	95%

Figure 7: Authentication success rate for PIN, password, Picture Password and Awase-E

Again as expected, Figure 7 shows that Awase-E has the highest authentication success rate, recording a 90% success rate in Stage 1 and 95% both in Stage 2 and 3. PIN and password were expected to decline in success rate and did so with PIN doing better than password, scoring 75% and 65% success rate in Stage 3, respectively. It is interesting to note that Awase-E performed more poorly than the other techniques in Stage 1 where two participants made the mistake of missing their pass-image and pressing the no pass-image button.

Picture Password, on the other hand performed as expected with a high success rate, rating equally as well as the PIN and password techniques in Stages 1 and 2. Picture Password was expected to score a higher success rate in Stage 3 but dropped significantly to 55% - i.e. almost half of all the participants got their pass-image incorrect.

While no performance data have been published for Picture Password, it seems that its performance in terms of success rate did as poorly as its speed of authentication. As for Awase-E, its success rate results in this experiment is consistent with reported performance where it has been shown to maintain a high authentication success rate as over time (Takada et al. 2006), reaching as high as 100% success rate even after a period of 16 weeks. However, there's a difference between Awase-E (Takada et al. 2006) interpreted a successful authentication compared to this report. In the research (Takada et al. 2006), the participant is allowed 3 trials for all authentication techniques and if participants succeeded within 3 trials then the attempt was considered successful. In contrast, this current research regards successful first trial or attempt as successful authentication and thus the findings from the two reports are not directly comparable.

The results indicate that Awase-E could improve authentication rates among users and could potentially serve as an alternative security measure to PIN and password while users may be reluctant to use Picture Password due to the high chance of authentication failure. However, it is important to note that even though PIN and password did poorly compared to Awase-E, users may still prefer to use the former techniques due to familiarity. By crossing the authentication success rate data with participant survey, at least 35% of the participants rated PIN or

password as their preferred technique (Top 1 and 2) despite making an error while using PIN or password in Stage 3 (Refer to Table 5).

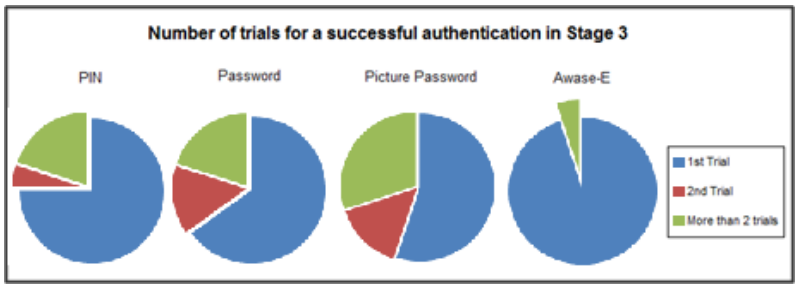


Figure 8: Number of trials for PIN, password, Picture Password and Awase-E

As users are more prone to authentication failure as time increases, for example in Stage 3, it is also worth looking at how many times participants need to re-authenticate when they made an error because users who made a mistake in the first trial but succeeded in the second trial may be willing to continue using the technique. However, if the user needs to re-authenticate more than twice, the user may feel that the authentication technique is being too obtrusive, leading to users disabling authentication.

Table 2. Number of trials for PIN, password, Picture Password and Awase-E

Stage 3	**PIN**	**Password**	**Picture Password**	**Awase-E**
1st Trial	75%	65%	60%	95%
2nd Trial	5%	15%	10%	0%
More than 2 trials	20%	20%	30%	5%

Figure 8 and Table 2 shows that PIN, password and Picture Password recorded 5%, 15% and 10% second trials, respectively while Awase-E had no second trials. Surprisingly, the number of participants requiring at least a third trial is more than the participants requiring only 2 trials in all four techniques, with PIN and password recording 20% of more than 2 trials each, while Picture Password and Awase-E recorded 30% and 5% correspondingly. Again, Awase-E has exceeded the performance of Picture Password in this aspect.

Table 3. Type of error and mistake made by participants

Error/Mistake	**0 Week**	**1 Week**
Picture too small	10	3
Confused with sequence	6	7
Input error	4	2
Recall error	3	10
Touch screen unresponsive	9	2
Unfamiliar with touch screen	4	1
Double clicked	1	0

Lastly, Table 3 shows the type of error made by the participants could also reveal areas for improvement of the IBA methods. The resulting authentication success rate could be due to one of the problems, errors or mistakes. Included among these are the users being confused with the sequence of either PIN or Picture Password, input errors and most importantly, recall errors which increased from 3 to 10 occurrences after one week. Notably, sequence and recall errors had the strongest effect on the authentication success rate. However, further research is needed to identify which technique is more prone to which type of error and which ones matter the most to the users.

User behaviour and opinions towards mobile security and IBA

When asked how many times the participant is willing to be authenticated in a day, 15% answered not at all, 40% only once during power on, 25% several times in a day and 20% every time they access the phone (Refer to Table 4). This means in total, at least 85% of the participants are willing to use authentication security on their mobile phones. However, the data collected were not significant enough to be analysed in terms of authentication frequency preference according to usage groups. Future research can be done to focus on this area.

Table 4. Usage per day against number of willing authentication

Phone Usage Per Day	**None**	**Once**	**Several**	**Every time**	**Total**
1 to 5	1	4	1	1	35%
5 to 10	2	3	0	1	30%
More than 10	0	1	4	2	35%
Total	15%	40%	25%	20%	100%

Although all of the participants were aware of some sort of security mechanism on their phone such as power on PIN, SIM lock or standby lock, only 35% used them quoting the need to protect data and email accounts from unintended use and in case the phone was lost. The remaining 65% of the participants either did not know how to set up a PIN or password lock or were reluctant to use it giving reasons such as that it was unnecessary, not having significant data stored, troublesome, disabled by default, too time consuming for frequent access to phone. Some users were very particular about their phones and had never let other people use them.

While more than half of the participants are not currently using any mobile security mechanism on their phone, the survey in this experiment showed that, with increased awareness, users may be willing to adopt some sort of authentication mechanism to protect their phone, IBA being one of them.

User preference of the experimented authentication techniques

Table 5. Preference of PIN, password, Picture Password and Awase-E

Preference	**PIN**		**Password**		**Picture Password**		**Awase-E**	
	0 Week	1 Week	0 Week	1 Week	0 Week	1 Week	0 Week	1 Week
Top 1	15%	25%	20%	35%	25%	0%	45%	40%
Top 2	45%	50%	45%	55%	45%	30%	70%	65%

Table 5 illustrates the preference on PIN increasing over the duration of the experiment could be due to the fact that it has a higher speed for authentication and also higher authentication success rate. However, surprisingly, the preference for password also increased although the technique performed poorly in terms of speed and authentication success rate. The only possible explanation for this is that password remains as the more familiar authentication technique and users are not ready to give it up completely and opt for newer authentication systems. Follow up questionnaires could explore this premise further. Finally, as expected, the poor performance by Picture Password results in a significant drop in preference. Interestingly, Awase-E managed to maintain a preference rating despite experiencing a slight drop towards the end of the experiment.

Problems and Improvements for Picture Password

Initially, Picture Password was notably a top favourite for at least 25% of the participants. However, this declined sharply after one week where none of the participants rated it as their top preferred authentication method. Apart from finding the method confusing and hard to remember, participants were having trouble finding or locating their pass-images, resulting in high error rates and slow authentication speed.

Participants suggested that this technique could be improved if the pass-image sequence restriction were lifted, enabling the users to input whichever selected pass-images they saw first, followed by the remainder of the pass-images. This is, of course a probable solution to improve authentication speed and success rate. However, users may instead need to remember which pass-image has been inputted to avoid inputting the same pass-image more than once. In addition, the implication on the technique's entropy may need to be studied.

Problems and Improvements for Awase-E

Many participants stated that they might use Awase-E and that the technique could improve security. In fact, Awase-E was highly preferred throughout the experiment, recording 45% top favourite despite dropping slightly to 40% towards the end of the experiment.

Participants suggested that the Awase-E technique should allow pass-images to be selected from the photo collection already residing in their phone. This was a plausible function as seen in Awase-E research report (Takada et al. 2006) where users can upload their personal photographs to be used as a pass-image to an Awase-E server from either a computer or a mobile phone. However, due to the nature of this experiment, the data from all participants needed to be centralized thus, participants were asked to create an ad hoc and simple pass-image using the camera function on the mobile phone used in this experiment.

Improvements for both IBA techniques

From the author's observation during the experiment sessions, there are also several UI improvements that both Picture Password and Awase-E can adopt.

(a) Larger image for user input – Some participants have big fingers especially the thumb which often blocks the image button the participant is trying to press. The smaller image button used has caused participants to accidently select the wrong image.

(b) Larger gaps between buttons or images could improve user's perception of the precise location of the image. Other than that, accidental pressing of adjacent buttons or images can also be avoided.

(c) Button or image press event – A "click" event requires a user to press and release the same button to complete the event. Often participants' button clicks were cancelled because they failed to complete the second part of the click event, releasing their presses on the same button. Instead, participants' presses were released away from the button they were trying to click. In order to solve this, images or buttons should use the "keydown" event rather than the "click" event where the UI can detect inputs instantly when the user presses the button.

CONCLUSION

Mobile phones are becoming increasingly important and valuable but the current authentication techniques of PIN and password are often misused resulting in unprotected information in the phones. While other authentication methods such as tokens and biometrics exist, they have well known limitations that may hinder user adoption. Alternatively, image-based authentication (IBA) shows promising results in relation to improved memorability.

This paper conducted an experiment to compare two IBA techniques, Picture Password and Awase-E in terms of their usability, performance and user opinions towards the techniques in order to answer three research questions: Which IBA technique authenticates faster, which IBA technique has a higher authentication success rate, and what the user opinions are towards the IBA techniques. The key findings show that PIN authenticates the fastest, followed by Awase-E, while Awase-E shows higher authentication success rate followed by PIN. Both Awase-E and PIN are rated the highest in terms of user preference among the experimented authentication techniques. The findings have been presented and discussed along with proposed improvements for the IBA techniques.

The paper contributes towards the body of knowledge in user authentication especially in the usability study of IBA techniques for authentication purposes in general by providing an indication of the usability of IBA techniques and proposing improvements that can enhance the authentication experience, thus encouraging consumers to increase adoption of IBA for their mobile phones and other devices.

The main limitation with this research is the sample size. The small sample size may result in misrepresentation of the performance of the IBA techniques for the whole population. Despite the limitations, this paper serves as an exploratory endeavour to provide indications of the usability, performance and user opinions towards IBA and also identifies potential directions for future research. Another limitation is the representativeness of the experiment, in that it does not represent a real life usage scenario, i.e. a user choosing a PIN to be used in his or her phone in real life might result in higher memorability than the experimental scenario in this paper.

Thus, future research based on a larger sample size, can explore other statistical values such as standard deviation. Other factors such as age, gender or social group can also be taken into consideration for analysis. There was no one best technique that performed excellently across all aspects investigated in this experiment. However, it can be concluded that apart from PIN and password, that were included in the experiment as control techniques, between Picture Password and Awase-E, the latter outperformed the former significantly in terms of authentication speed and success rate and is thus worthy of further investigation and improvements. Therefore,

further research is proposed for investigating what and which user acceptance criteria are the most important for mobile authentication and how IBA, especially Awase-E, performs in terms of the identified criteria. For example, one of the criteria could be pass-image creation time which may be investigated by allowing Awase-E to select pass-images from the user's own photo gallery in the phone. The performance of Picture Password without implementing sequence restriction is also an interesting avenue for future study. Distributed data gathering software could also be developed to gather performance data on real users mobile phones in a real life usage scenarios. Lastly, it is also important to investigate the types of errors that the IBAs are prone to, which matter the most to users and how they can be improved.

REFERENCES

Adams, A., and Sasse, M. 1999. "Users Are Not the Enemy," *Commun. ACM* (42:12), pp 40-46.

Adams, A., Sasse, M., and Lunt, P. 1997. "Making Passwords Secure and Usable," *People and Computers*), pp 1-20.

Clarke, N., and Furnell, S. 2005. "Authentication of Users on Mobile Telephones–a Survey of Attitudes and Practices," *Computers & Security* (24:7), pp 519-527.

De Angeli, A., Coventry, L., Johnson, G., and Coutts, M. 2003. "Usability and User Authentication: Pictorial Passwords Vs. Pin," *Contemporary Ergonomics*), pp 253-258.

Dhamija, R., and Perrig, A. 2000. "Deja Vu: A User Study Using Images for Authentication," pp. 45-48.

Furnell, S.M., and Clarke, N.L. 2007. "Advanced User Authentication for Mobile Devices," *Computers & Security* (26:2), pp 109-119.

Grashey, S., and Schuster, M. 2006. "Multiple Biometrics," *SmartKom: Foundations of Multimodal Dialogue Systems*), pp 181-193.

Jansen, W. 2004. "Authenticating Mobile Device Users through Image Selection," *The Internet Society: Advances in Learning, Commerce and Security* (1), pp 183-194.

Jermyn, I., Mayer, A., Fabian Monrose, Z., Reiter, M., and Rubin, A. 1999. "The Design and Analysis of Graphical Passwords," Citeseer, pp. 1-14.

Nicholson, A.J., Corner, M.D., and Noble, B.D. 2006. "Mobile Device Security Using Transient Authentication," *IEEE Transactions on Mobile Computing* (5:11), pp 1489-1502.

O'Gorman, L. 2003. "Comparing Passwords, Tokens, and Biometrics for User Authentication," *Proceedings of the IEEE* (91:12), pp 2021-2040.

Phifer, L. 2008. "Mobile Security: Protecting Mobile Devices, Data Integrity and Your Corporate Network," *Search Mobile Computing*).

Takada, T., and Koike, H. 2003. "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images," *Lecture Notes in Computer Science*), pp 347-351.

Takada, T., Onuki, T., and Koike, H. 2006. "Awase-E: Recognition-Based Image Authentication Scheme Using Users' Personal Photographs," *Innovations in Information Technology, 2006*), pp 1-5.

Weiss, R., and Luca, A.D. 2008. "Passshapes: Utilizing Stroke Based Authentication to Increase Password Memorability," in: *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. Lund, Sweden: ACM.

COPYRIGHT